UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/780,252	02/17/2004	Pratyush Moghe	TIZOR-001	9651

50086 7590 10/27/2010

LAW OFFICE OF DAVID H. JUDSON
15950 DALLAS PARKWAY
SUITE 225
DALLAS, TX 75248

EXAMINER	
JUNG, DAVID YIUK	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
10/27/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mail@davidjudson.com

Office Action Summary	Application No.	Applicant(s)	
	10/780,252	MOGHE, PRATYUSH	
	Examiner	Art Unit	
	David Y. Jung	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *8/23/2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) *1-29,42-45,47-49,52 and 53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-29,42-45,47-49,52 and 53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

CLAIMS PRESENTED

Claims 1-29, 42-45 and 47-49, 52-53 are presented.

Claims 52-53 are new.

Response to Applicant's Request for Interview

Applicant's representative has been contacted three times after USPTO received his response to the previous Office Action. Applicant's representative has been contacted on September 30, 2010. Applicant's representative stated that he was not prepared to discuss the case. Applicant's representative was telephoned on October 5 and PTO left a message asking when the representative shall be available. Then, Applicant's representative was again (on October 6) telephoned and again was left with the same message. Thus, Applicant's representative has been contacted three times but the representative has not responded except to note that he is not currently prepared to discuss the case. Applicant's representative has not provided a future time in which he will be prepared to discuss the case. After October 9, the examination for this case began without his participation.

Response to Arguments

Applicant's arguments filed have been fully considered but they are not persuasive. Applicant states: "These claims include wording similar to that proposed by the Examiner, namely the phrase indicating that the method

'examines an entirety of an application laver without any application-specific limits.' The Examiner is requested to indicate whether this proposal formulation would be acceptable, and the Examiner is thanked in advance for his consideration." This is a misinterpretation of the Office Action. Applicant is respectfully requested to note that the sentence was in the context of other sentences of specification: "There have been earlier applications of anomaly detection, but for lower-level activities such as intrusion detection (network-layer or system-layer), or for specific application activity monitoring such as transaction monitoring (credit cards). Information content layer activities are much broader and complex than network-layer or system-layer activities."

Applicant asserts that the prior art did not specifically mention the features[1]. Yet, "[t]here have been earlier applications of anomaly detection, but for lower-level activities such as intrusion detection (network-layer or system-layer), or for specific application activity monitoring such as transaction monitoring (credit cards) (emphasis added)". The dependent claims recite exactly the features that were asserted as prior art by this sentence. Hypothetically, if Applicant wishes to amend the specification so as to not mean the meaning of this sentence or if Applicant wishes to delete passages of specification, then Applicant may do so as long as Applicant is willing to accept the

[1] Applicant asserts as follows in the second page of the Remarks. To establish anticipation, every element and limitation of the claimed invention must be found in a single prior art reference, arranged as in the claim. Karsten *Mfg.* Corp. v. Cleveland GolfCo., 242 F.3d 1376, 1383 (Fed. Cir. 2001) "Absence from the reference of any claimed element negates anticipation." Kloster Speedsteel AB v. Crucible, Znc., 793 F.2d 1565, 1571 (Fed.Cir.1986). Here, and with respect, the Examiner has not shown how either claim 1 or claim 49 is anticipated. Further, the Applicant has not admitted that the subject matter of the dependent claims is admitted prior art.

consequences of 35 USC 112 1st paragraph regarding such hypothetical changes to the specification.

Allowable Subject Matter

The following is a statement of reasons for the indication of allowable subject matter: Applicant's claims have been amended enough to be able to guess at (but not actually know for sure) what may be allowable upon additional features. Page 5 of the specification is singled out as succeeding to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Yet, none of the claims have yet to claim any of this subject matter. The page 5 of the specification provides:

The invention is unique in two respects -1. Technology: Monitoring and analysis is based on trending and anomaly detection at the information or content-level. There have been earlier applications of anomaly detection, but for lower-level activities such as intrusion detection (network-layer or system-layer), or for specific application activity monitoring such as transaction monitoring (credit cards). Information content layer activities are much broader and complex than network-layer or system-layer activities. 2. Application: The current invention has several unique risk assessment applications in the information content security arena. a. Unauthorized Information Disclosure: The invention can detect anomalies based on correlation of information flow, users, and time. These anomalies can be used to discover "unauthorized information disclosures" from confidential information repositories, without requiring to know the specific type of information being disclosed. b. Content Usage Analysis: The invention can analyze content usage and classify content based on rare information exchanges versus common and widely shared information exchanges. This can lead to discovery of "critical" information assets within the organization.

Yet, none of the claims have yet to claim any of this subject matter. Merely claiming "application layer" would directly lead to being covered by "specific application activity monitoring" which is clearly a prior art according to page 5 (and according to

actual facts of the art of security). The claims need to recite "entirety of application layer, said entirety of application layer without any application-specific limits."

The art listed in the specification (at the bibliography in the last pages) amply and redundantly show that prior art did indeed (well known even without page 5 of the specification) already have the Unauthorized Information Disclosure and the Content Usage Analysis as also noted in page 5. Because the prior art did indeed (well known even without page 5) already have the Unauthorized Information Disclosure and the Content Usage Analysis as also noted in page 5, the claims can never be allowed without overcome the admissions against art at page 5 of the specification of this application. Thus: merely claiming "application layer" would directly lead to being covered by "specific application activity monitoring" which is clearly a prior art according to page 5 (and according to actual facts of the art of security). The claims need to recite "entirety of application layer, said entirety of application layer without any application-specific limits." At the moment, none of the claims have yet to claim any of this subject matter.

Thus, at the minimum (even if not sufficient, at least necessary) the indicated subject matter would be:

1. A method of performing an application layer semantic analysis to monitor and to detect information access anomalies, the semantic analysis to analyze the anomalies for unauthorized information disclosures from confidential information repositories, requiring to know the specific type of information being disclosed, the semantic analysis to analyze content usage and classify content based on rare information exchanges

versus common and widely shared information exchanges so as to discovery of "critical" information assets within the organization,

comprising:

a) capturing data packets;

b) monitoring the captured packets at an information or at an content-level

c) filtering the captured data packets to detect information content;

d) processing packets at the information or content-level based on semantics of an application or protocol;

e) generating a quantitative representation;

f) deriving a content signature from the quantitative representation;

g) deriving a prototypical model based at least on correlation of information flow, users, and time, said model includes a frequency view of a set of content signatures accessed by a given user, where the set of content signatures are indicative of content that is changing over time; and

h) detecting an application layer information access anomaly at the information or content-level by using a semantic analysis to detect a given deviation from the prototypical model, wherein said application layer is the level higher than network layer in which one or more of intrusion detection occurs, is the level higher than system layer in which one or more of the intrusion detection occurs,

i) assessing security risk of applications at the information or content-level information content; and

j) monitoring the detected anomalies for unauthorized information disclosures from confidential information repositories.

CLAIM REJECTIONS

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action.

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-29, 42-45 and 47-49, 52-53 are rejected under 35 U.S.C. 102 (a) as being clearly anticipated by admissions over the prior arts. For claims 1-29, 42-45 and 47-49, see the previous Office Actions. The claims and the rejections remain unchanged.

Regarding claims 52, 53, Applicant added limitations "examines an entirety of an application laver without any application-specific limits." Applicant explains these claims 52, 53. Applicant states: "These claims include wording similar to that proposed by the Examiner, namely the phrase indicating that the method 'examines an entirety of an application laver without any application-specific limits.' The Examiner is requested to indicate whether this proposal formulation would be acceptable, and the Examiner is thanked in advance for his consideration." This is a misinterpretation of the Office

Action. Applicant is respectfully requested to note that the sentence was in the context of other sentences of specification: "There have been earlier applications of anomaly detection, but for lower-level activities such as intrusion detection (network-layer or system-layer), or for specific application activity monitoring such as transaction monitoring (credit cards). Information content layer activities are much broader and complex than network-layer or system-layer activities."

Applicant asserts that the prior art did not specifically mention the features[2]. Yet, "[t]here have been earlier applications of anomaly detection, but for lower-level activities such as intrusion detection (network-layer or system-layer), or for specific application activity monitoring such as transaction monitoring (credit cards) (emphasis added)". The dependent claims recite exactly the features that were asserted as prior art by this sentence.

Conclusion

[2] Applicant asserts as follows in the second page of the Remarks. To establish anticipation, every element and limitation of the claimed invention must be found in a single prior art reference, arranged as in the claim. Karsten *Mfg.* Corp. v. Cleveland GolfCo., 242 F.3d 1376, 1383 (Fed. Cir. 2001) "Absence from the reference of any claimed element negates anticipation." Kloster Speedsteel AB v. Crucible, Znc., 793 F.2d 1565, 1571 (Fed.Cir.1986). Here, and with respect, the Examiner has not shown how either claim 1 or claim 49 is anticipated. Further, the Applicant has not admitted that the subject matter of the dependent claims is admitted prior art.

The art made of record and not relied upon is considered pertinent to applicant's disclosure. The art disclosed general background.

1. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Points of Contact

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, D.C. 20231

or faxed to:

(571) 273-8300, (for formal communications intended for entry)

Or:

(571) 273-3836 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David Jung whose telephone number is (571) 272-3836 or William Korzuch whose telephone number is (571) 272-7589.

/David Y Jung/

Primary Examiner of Art Unit 2431

David Jung

David Jung

Patent Examiner

10/25/10